Matematik, KTH
B.Ek

Lösningar tentan SF1662 DISKRET MATEMATIK, 2 juni 2015

Tryckfel kan förekomma.

1) (3p) Vi söker alla $x \in \mathbb{Z}$ med $322x \equiv 28 \pmod{357}$.

Lösning: $322x \equiv 28 \pmod{357}$ är ekvivalent med att $322x + 357k = 28$ för något $k \in \mathbb{Z}$.
Euklides algoritm:

$$\begin{cases} 357 = 1 \cdot 322 + 35, \\ 322 = 9 \cdot 35 + 7, \\ 35 = 5 \cdot 7 + 0 \end{cases} \quad \text{så } \operatorname{sgd}(322, 357) = 7 \text{ och } \begin{cases} 7 = 322 - 9 \cdot 35 = \\ = 322 - 9(357 - 322) = \\ = 10 \cdot 322 - 9 \cdot 357 \end{cases}$$

Division med $\operatorname{sgd}(322, 357) = 7$ ger $46 \cdot 10 + 51 \cdot (-9) = 1$ medan den nya ekvationen blir ekvivalent med $46x + 51k = 4$.
Multiplikation med 4 ger $46 \cdot 40 + 51 \cdot (-36) = 4$, så $\begin{cases} x_0 = 40 \\ k_0 = -36 \end{cases}$ är en lösning.
x, k är då en lösning omm $46(x - x_0) + 51(k - k_0) = 0$, dvs (eftersom $\operatorname{sgd}(46, 51) = 1$, måste $51 \mid (x - x_0)$, så $x - x_0 = 51n$, $n \in \mathbb{Z}$, och alla $n \in \mathbb{Z}$ ger lösningar) $x - x_0 = 51n$ (och $k - k_0 = -46n$) för något $n \in \mathbb{Z}$.

Svar: Alla lösningar ges av $x = 40 + 51n$, där $n \in \mathbb{Z}$.

(Alternativt, med Eulers metod: $322x + 357k = 28$ ger $x = -k + \frac{28 - 35k}{322} = -k + z$, där $28 - 35k = 322z$, $z \in \mathbb{Z}$, så $k = -9z + \frac{28 - 7z}{35} = -9z + u$, där $28 - 7z = 35u$, $u \in \mathbb{Z}$, så $z = 4 - 5u$, $u \in \mathbb{Z}$ godtyckligt.
Det ger $k = -9(4 - 5u) + u = -36 + 46u$ och $x = -(-36 + 46u) + (4 - 5u) = 40 - 51u$ (så $u = -n$).
Alternativt, med moduloräkning: $322x \equiv_{357} 28 \Leftrightarrow 46x \equiv_{51} -5x \equiv_{51} 4$ (ty $357 = 7 \cdot 51 \mid (322x - 28) = 7 \cdot (46x - 4) \Leftrightarrow$ $\Leftrightarrow 51 \mid (46x - 4)) \Leftrightarrow -50x \equiv_{51} 40$ (ty $\operatorname{sgd}(10, 51) = 1$, så $51 \mid (-5x - 4) \Leftrightarrow 51 \mid 10 \cdot (-5x - 4)) \Leftrightarrow x \equiv_{51} 40$.)

---

2) Fibonacci-talen $\{F_n\}_{n=0}^{\infty}$ definieras av $F_0 = 0,\ F_1 = 1,\ F_{n+2} = F_{n+1} + F_n$ för $n \in \mathbb{N}$.
Vi skall för alla $n \in \mathbb{N}$ visa att $F_{n+1}F_{n+2} = F_nF_{n+3} + (-1)^n$.

Lösning: Med induktion visas påståendet $P_n : F_{n+1}F_{n+2} - F_nF_{n+3} = (-1)^n$ för alla $n \in \mathbb{N}$.
Bas: P_0 är sant, ty $\text{VL}_0 = F_1F_2 - F_0F_3 = F_1(F_0 + F_1) - 0 \cdot F_3 = 1 \cdot 1 - 0 = 1$, $\text{HL}_0 = (-1)^0 = 1$.
Steg: Antag P_k för ett godtyckligt $k \in \mathbb{N}$, dvs $F_{k+1}F_{k+2} - F_kF_{k+3} = (-1)^k$.
Då är $\text{VL}_{k+1} = F_{k+2}F_{k+3} - F_{k+1}F_{k+4} = (F_k + F_{k+1})F_{k+3} - F_{k+1}(F_{k+2} + F_{k+3}) = F_kF_{k+3} - F_{k+1}F_{k+2} \overset{\text{IA}}{=} -(-1)^k = (-1)^{k+1} = \text{HL}_{k+1}$.
Så om P_k är sant är P_{k+1} sant och **enligt induktionsprincipen är saken klar.**

---

3) (3p) Vi söker antalet sätt att (oordnat) välja ut 50 kulor bland 53 kulörta, särskiljbara, och 48 svarta, identiska kulor.

Lösning: Ett val bestäms helt av vilka vita kulor som är med, svarta fyller ut. För varje vit kula avgör man om den skall vara med eller inte. Det ger 2^{53} möjligheter, men omöjliga är fallen då vi valt 53, 52 eller 51 vita kulor (de blir för många) eller då vi bara valt en eller ingen vit kula (de svarta räcker inte för att fylla ut till 50 st). Dessa omöjliga fall dras bort.
53 vita kan väljas på ett sätt (alla med), 52 st på 53 sätt (vilken inte med?), 51 st på $\binom{53}{2} = \frac{53 \cdot 52}{2 \cdot 1} = 26 \cdot 53$ sätt (vilka inte med?), en enda på 53 sätt (vilken?) och ingen på 1 sätt (ingen med).
Det sökta antalet blir alltså $2^{53} - 1 - 53 - 26 \cdot 53 - 53 - 1 = 2^{53} - 26 \cdot 53 - 108$.

Svar: 50 kulor kan väljas på $\mathbf{2^{53} - 26 \cdot 53 - 108 (= 9\,007\,199\,254\,739\,506)}$ sätt.

---

4) G är en ändlig grupp, $g \in G$ uppfyller $g^{51} = 1 \neq g^{15}$ och G har en delgrupp H med $|H| = 25$. Vi söker (a, 2p) möjliga värden för $o(g)$ och (b, 1p) minsta möjliga värde för $|G|$.

Lösning: a. $g^{51} = 1$ ger att $o(g) \mid 51$ (känd sats), så $o(g)$ är någon av 1, 3, 17, 51. Men $g^{15} = (g^3)^5 \neq 1$, så $g^3 \neq 1$ och $o(g) \neq 1, 3$.
b. Då $g \in G$ och H är en delgrupp till G gäller (från Lagranges sats) $o(g) \big| |G|$ och $|H| \big| |G|$, så $17, 25 \big| |G|$ och ($\text{mgm}(17, 25) = 17 \cdot 25 = 425$, ty $\operatorname{sgd}(17, 25) = 1$) $425 \big| |G|$. $|G| > 0$ ger $|G| \geq 425$.
Exemplet $G = \langle x \rangle$, $o(x) = 425$ med $g = x^{25}$, $H = \langle x^{17} \rangle$ visar att $o(g) = 17$ och $|G| = 425$ är möjliga. $G = \langle x \rangle$, $o(x) = 1275$ med $g = x^{25}$, $H = \langle x^{51} \rangle$ visar att $o(g) = 51$ är möjligt.

Svar a: $o(g) = 17$ eller 51, b: $|G|$:s minsta möjliga värde är 425.

---

5) (3p) Den ena av grafen $G = (V, E)$:s två komponenter är isomorf med en plan graf vars dualgraf är isomorf med den andra komponenten. Vi söker $e(= |E|)$, då $v(= |V|)$ är känd.

Lösning: Låt den i:e komponenten ($i = 1, 2$) plant ritad ha v_i hörn, e_i kanter och r_i ytor. Då är $v = v_1 + v_2$ och $e = e_1 + e_2$. I varje yta till en plan graf finns precis ett av dualgrafens hörn, så $r_1 = v_2$. Eulers polyederformel för en plan, sammanhängande graf ger $v_1 - e_1 + r_1 = 2$, så $v_1 - e_1 + v_2 = v - e_1 = 2$ och $e_1 = v - 2$. Men $e_2 = e_1$ (varje kant i en plan graf och dess dualgraf korsar precis en kant i den andra), så $e = e_1 + e_2 = 2e_1 = 2v - 4$.

Svar: Antalet kanter är $e = 2v - 4$.

---

6) Vi söker (minsta icke-negativa) resten då $2^{6^{2015}}$ divideras med (a, 1p) 19 och (b, 3p) 23.

Lösning: De sökta resterna är $x \equiv_p 2^{6^{2015}}$, $0 \leq x < p$ för $p = 19, 23$.
a. Fermats lilla sats ger att $2^{18} \equiv_{19} 1$ (ty $18 = 19 - 1$, 19 är ett primtal och $19 \nmid 2$),
så $2^{6^{2015}} = 2^{6^2 \cdot 6^{2013}} = ((2^{18})^2)^{6^{2013}} \equiv_{19} 1$.
b. Fermat ger som nyss att $2^{22} \equiv_{23} 1$.
$22 = 2 \cdot 11$, så $6^{10k+1} \equiv_{22} 6$ för $k \in \mathbb{N}$ (enligt satsen bakom RSA; 2 och 11 primtal, $10 = (2-1)(11-1)$).
Det ger $6^{2015} = 6^{201 \cdot 10 + 1} \cdot 6^4 \equiv_{22} 6 \cdot 6^4 = 6 \cdot 36^2 \equiv_{22} 6 \cdot (-8)^2 \equiv_{22} 6 \cdot (-2) \equiv_{22} 10$.
För ett $n \in \mathbb{N}$ är alltså $2^{6^{2015}} = 2^{22n+10} \equiv_{23} 1^n \cdot 2^{10} = 32^2 \equiv_{23} 9^2 = 81 \equiv_{23} 12$.

Svar: De sökta resterna blir a: 1 och b: 12.

---

7) Permutationen $\pi \in S_9$ ges av att $\pi(1) = 7$, $\pi(2) = 8$, $\pi(3) = 2$, $\pi(4) = 4$, $\pi(5) = 5$, $\pi(6) = 9$, $\pi(7) = 1$, $\pi(8) = 3$, $\pi(9) = 6$. Vi söker (a, 1p) π i cykelnotation och dess ordning $o(\pi)$ och (b, 3p) $\sigma_1, \sigma_2 \in S_9$ med $o(\sigma_1\pi) > o(\pi) > o(\sigma_2\pi) > 1$.

Lösning: a. $\pi(1) = 7$, $\pi(7) = 1$, $\pi(2) = 8$, $\pi(8) = 3, \ldots$ ger $\pi = (1\,7)(2\,8\,3)(6\,9)$.
Dess ordning är mgm av cykellängderna, $o(\pi) = \text{mgm}(2, 3, 1, 1, 2) = 6$.
b. $\sigma_1\pi$ och $\sigma_2\pi$ kan vara godtyckliga i S_9 med rätta ordningar. Man kan t.ex. välja $\sigma_1\pi = (1\,7\,6\,9)(2\,8\,3)$ med $o(\sigma_1\pi) = \text{mgm}(4, 3) = 12$ och $\sigma_2\pi = (2\,8\,3)$ med $o(\sigma_2\pi) = 3$.
Just de valen ger $\sigma_1 = (\sigma_1\pi)\pi^{-1} = (1\,7\,6\,9)(2\,8\,3)(1\,7)(2\,3\,8)(6\,9) = (1\,6)$ och
$\sigma_2 = (\sigma_2\pi)\pi^{-1} = (2\,8\,3)(1\,7)(2\,3\,8)(6\,9) = (1\,7)(6\,9)$.

Svar a: $\pi = (1\,7)(2\,8\,3)(6\,9)$ och $o(\pi) = 6$, b: T.ex. $\sigma_1 = (1\,6)$, $\sigma_2 = (1\,7)(6\,9)$.

---

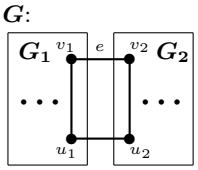
8) $(U_{1001}, \cdot)$ är gruppen av inverterbara element i $\mathbb{Z}_{1001}$. Vi skall (a, 2p) finna $|U_{1001}|$, (b, 1p) visa att (för $x, y \in \mathbb{Z}$) $x \equiv y \pmod{1001} \Leftrightarrow x \equiv y \pmod{m}$ för alla tre $m = 7, 11, 13$ och (c, 1p) avgöra om $(U_{1001}, \cdot)$ är en cyklisk grupp.

Lösning: a. $x \in \mathbb{Z}_{1001}$ är inverterbart omm $\text{sgd}(x, 1001) = 1$, så omm $7, 11, 13 \nmid x$.
$|U_{1001}|$ kan fås med inklusion/exklusion. Låt (för $m = 7, 11, 13$) $A_m = \{x \in \mathbb{Z}_{1001} \mid m \text{ delar } x\}$.
Då är $|A_m| = \frac{1001}{m}$, $|A_{m_1} \cap A_{m_2}| = \frac{1001}{m_1 \cdot m_2}$ (då $m_1 \neq m_2$) och $|A_7 \cap A_{11} \cap A_{13}| = |\{0\}| = 1$, så
$|U_{1001}| = |\mathbb{Z}_{1001} \setminus (A_7 \cup A_{11} \cup A_{13})| = 1001 - (\frac{1001}{7} + \frac{1001}{11} + \frac{1001}{13}) + (13 + 11 + 7) - 1 =$
$= 7 \cdot 11 \cdot 13 - (11 \cdot 13 + 7 \cdot 13 + 7 \cdot 11) + (13 + 11 + 7) - 1 = (7-1)(11-1)(13-1) = 6 \cdot 10 \cdot 12 = 720$.
b. $x \equiv y \pmod{1001} \Leftrightarrow 1001 = 7 \cdot 11 \cdot 13 \mid (x - y) \Leftrightarrow 7, 11, 13 \mid (x - y)$ (ty 7, 11 och 13 är parvis relativt prima, så primfaktoriseringen av $x - y$ måste innehålla dem alla om de delar $x - y$).
c. Att $x \in \mathbb{Z}_{1001}$ är inverterbart betyder att det finns $y \in \mathbb{Z}$ sådant att x som element i $\mathbb{Z}$ uppfyller $x \cdot y \equiv_{1001} 1$, så (enligt b.) $x \cdot y \equiv_m 1$ för $m = 7, 11, 13$. Speciellt är $x \not\equiv_m 0$, så (Fermats lilla sats, 7, 11, 13 är primtal) $x^6 \equiv_7 1$, $x^{10} \equiv_{11} 1$, $x^{12} \equiv_{13} 1$ och därmed $x^{60} \equiv_{7,11,13} 1$, så $x^{60} \equiv_{1001} 1$ och $o(x)$ i U_{1001} delar 60 och är speciellt $\neq 720$. Gruppen är alltså inte cyklisk.

Svar a: $|U_{1001}| = 720$, b: Visat ovan, c: Nej, den är inte cyklisk.

---

9) (5p) Vi söker kromatiska polynomet $P_G(\lambda)$ för grafen $G = (V, E)$ som fås från graferna $G_1 = (V_1, E_1)$ och $G_2 = (V_2, E_2)$ (med $V_1 \cap V_2 = \varnothing$) enligt $V = V_1 \cup V_2$, $E = E_1 \cup E_2 \cup \{\{u_1, u_2\}, \{v_1, v_2\}\}$ (där $\{u_1, v_1\} \in E_1$ och $\{u_2, v_2\} \in E_2$), givet de kromatiska polynomen $P_{G_1}(\lambda)$, $P_{G_2}(\lambda)$.



Lösning: Vi låter $e = \{v_1, v_2\}$ och använder rekursionsformeln för kromatiska polynom, $P_G(\lambda) = P_{G-e}(\lambda) - P_{G/e}(\lambda)$ (med gängse beteckningar).
Hörnfärgningar av $G - e$ motsvarar precis dem av först G_1 och sedan G_2, med den enda inskränkningen att u_1 och u_2 måste ges olika färger. För var och en av de $P_{G_1}(\lambda)$ olika färgningarna av G_1 kan då G_2 färgas på $(1 - \frac{1}{\lambda})P_{G_2}(\lambda)$ sätt (otillåtna är andelen $\frac{1}{\lambda}$ av alla G_2-färgningar, de där u_2:s färg = u_1:s), så $P_{G-e}(\lambda) = \frac{\lambda-1}{\lambda} P_{G_1}(\lambda) \cdot P_{G_2}(\lambda)$.
Hörnfärgningar av G/e motsvarar också dem av först G_1 och sedan G_2, men nu med inskränkningarna att v_1 och v_2 skall ha samma färg och u_1 och u_2 olika. För var och en av de $P_{G_1}(\lambda)$ olika färgningarna av G_1 kan nu G_2 färgas på $\frac{1}{\lambda}(1 - \frac{1}{\lambda-1})P_{G_2}(\lambda)$ sätt (av andelen $\frac{1}{\lambda}$ G_2-färgningar med v_2:s färg = v_1:s är andelen $\frac{1}{\lambda-1}$ förbjudna, nämligen de som har u_2:s färg = u_1:s (för båda är nu bara $\lambda - 1$ färger tillgängliga), så $P_{G/e}(\lambda) = \frac{\lambda-2}{\lambda(\lambda-1)} P_{G_1}(\lambda) \cdot P_{G_2}(\lambda)$.
Så $P_G(\lambda) = P_{G-e}(\lambda) - P_{G/e}(\lambda) = (\frac{\lambda-1}{\lambda} - \frac{\lambda-2}{\lambda(\lambda-1)})P_{G_1}(\lambda) \cdot P_{G_2}(\lambda) = \frac{\lambda^2-3\lambda+3}{\lambda(\lambda-1)} P_{G_1}(\lambda) \cdot P_{G_2}(\lambda)$.

Svar: Det kromatiska polynomet är $P_G(\lambda) = \frac{\lambda^2-3\lambda+3}{\lambda(\lambda-1)} \cdot P_{G_1}(\lambda) \cdot P_{G_2}(\lambda)$.

---

10) En kub smyckas med en färgad kula i varje hörn, så att antalen blå och röda kulor båda är 1 eller 2. Vi söker (a, 1p) antalet av kubens rotationssymmetrier och (b, 4p) antalet väsentligt olika sådana färgningar.

Lösning: Vi kallar kubens rotationssymmetrigrupp för G.
a. Om x är ett hörn är $|Gx| = 8$ (x:s bana består av alla hörnen) och $|G_x| = 3$ (precis 3 olika $g \in G$ uppfyller $gx = x$), så $|G| = |Gx| \cdot |G_x| = 24$ (känd sats).
b. Vi använder Burnsides lemma, så det sökta antalet är $\frac{1}{|G|} \sum_{g \in G} |X_g|$, där $|X_g|$ är antalet färgningar som inte ändras då g verkar (roterar kuben).

rotations-vinkel	axel genom	antal g	hörnens banor	$\lvert X_g \rvert$
0	—	1	$[1^8]$	$\lvert X_{id} \rvert$, se nedan
$\frac{2\pi}{3}$	hörn	8	$[1^2 3^2]$	$2 \cdot k^2$ (vilken röd? andra blå, två 3-banor)
π	sidmitt	3	$[2^4]$	$4 \cdot 3 \cdot k^2$ (vilket par rött? vilket blått? två par till)
$\frac{\pi}{2}$	sidmitt	6	$[4^2]$	0 (ingen hörnbana med 1 eller 2 st)
π	kantmitt	6	$[2^4]$	$4 \cdot 3 \cdot k^2$ (som ovan)

(Alla rotationsaxlarna går förstås genom kubens mittpunkt.)

$$|X_{id}| = \underbrace{8 \cdot 7 \cdot k^6}_{\text{1 röd, 1 blå}} + 2 \cdot \underbrace{\tbinom{8}{2} \cdot 6 \cdot k^5}_{\text{2 ena, 1 andra}} + \underbrace{\tbinom{8}{2} \cdot \tbinom{6}{2} \cdot k^4}_{\text{2 röda, 2 blå}} = 56k^6 + 2 \cdot 28 \cdot 6 \cdot k^5 + 28 \cdot 15 \cdot k^4 = 56k^6 + 336k^5 + 420k^4.$$

Antalet väsentligt olika färgningar blir alltså

$$\frac{1}{|G|} \sum_{g \in G} |X_g| = \frac{1}{24}(56k^6 + 336k^5 + 420k^4 + (8 \cdot 2 + 3 \cdot 12 + 6 \cdot 12)k^2 + 6 \cdot 0) = \frac{1}{24}(56k^6 + 336k^5 + 420k^4 + 124k^2).$$

Svar a: 24 st, b: $\frac{1}{24}(56k^6 + 336k^5 + 420k^4 + 124k^2)$ färgningar.
(För $k = 1$ blir antalet färgningar 39, för $k = 2$ blir det 898, för $k = 3$ blir det 6 567, för $k = 4$ blir det 28 456 etc.)
